8-10-2020

Design requirements for a cloud-based automated red team in a cyber range for security operations training

Justin Giboney
BYU, jgiboney@byu.edu

Kyle Adams
BYU, adamskyle@pm.me

William Atwood
BYU, willatwood95@yahoo.com

Joseph Belyeu
BYU, jcbelyeu@gmail.com

Caleb Crandall
BYU, cranman246@gmail.com

See next page for additional authors

Authors
Justin Giboney, Kyle Adams, William Atwood, Joseph Belyeu, Caleb Crandall, and Joshua Keller

Design requirements for a cloud-based automated red team in a cyber range for security operations training

TREO Talk Paper

Justin Giboney
Brigham Young University
justin_giboney@byu.edu

Kyle Adams, William Atwood, Joseph Belyeu, Caleb Crandall, Joshua Keller, Chelsia Liu, Dallin Olson, Nate Wilson
Brigham Young University

Abstract

Competitions for students, novices, and professionals to practice hacking and cyber defense skills (Conklin 2005; White et al. 2010). In cyber defense competitions teams design, implement, manage, and defend a network of computers and services (Schepens and James 2003). Cyber defense competitions are great learning opportunities for students and professionals. Typically, as in the case of the National Collegiate Cyber Defense Competition (https://www.nationalccdc.org/), the competitions consist of multiple blue teams of contestants and multiple red teams that attacks the services and systems that blue team is trying to counteract.

An automated attack system needs to be intelligent, have low overhead, be realistic, and be modular (Miller et al. 2018). The components of automated attack systems vary. A patent for a very high-level design of an automated penetration system uses simulators (virtual machines or software that mimics the behavior of computers or networks), an exploit database, storage for scenarios, configuration files, and a penetration testing framework (Futoransky et al. 2013). Other systems can simulate network and user traffic (Rossey et al. 2002).

We have so far identified four high-level design requirements: 1) ability to perform many types of attacks, 2) ability to follow a good process, 3) possession of a high-level situational understanding of the scenario, and 4) ease of sanitation and reuse of the simulation. Our continued work will identify more design requirements and areas of research that are needed to further the technological abilities and efficiency of automated red team design.

References (optional)

Conklin, A. 2005. "The Use of a Collegiate Cyber Defense Competition in Information Security Education," in *Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD '05*, pp. 16–18. (https://doi.org/10.1145/1107622.1107627).

Miller, D., Alford, R., Applebaum, A., Foster, H., Little, C., and Strom, B. 2018. "Automated Adversary Emulation: A Case for Planning and Acting with Unknowns." (https://www.mitre.org/sites/default/files/publications/pr-18-0944-1-automated-adversary-emulation-planning-acting.pdf).

Rossey, L. M., Cunningham, R. K., Fried, D. J., Rabek, J. C., Lippmann, R. P., Haines, J. W., and Zissman, M. A. 2002. "LARIAT: Lincoln Adaptable Real-Time Information Assurance Testbed," in *IEEE Aerospace Conference Proceedings*, pp. 2671–2682. (https://doi.org/10.1109/AERO.2002.1036158).

Schepens, W. J., and James, J. R. 2003. "Architecture of a Cyber Defense Competition," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics* (Vol. 5), pp. 4300–4305. (https://doi.org/10.1109/icsmc.2003.1245660).

White, G. B., Dwayne Williams, D. W., Keith, K., and Harrison, H. 2010. "The Cyberpatriot National High School Cyber Defense Competition," *IEEE Security & Privacy* (8:5), pp. 59–61.